AODV Routing Protocol Performance Analysis under MANET Attacks

Abdelshafy, M. & King, P. J. B.

Original citation & hyperlink:
Abdelshafy, M & King, PJB 2014, 'AODV Routing Protocol Performance Analysis under MANET Attacks' International Journal for Information Security Research (IJISR), vol. 4, no. 2, pp. 418-326.
https://dx.doi.org/10.20533/ijisr.2042.4639.2014.0048

DOI 10.20533/ijisr.2042.4639.2014.0048
ESSN 2042-4639

Publisher: Infonomics Society

AODV Routing Protocol Performance Analysis under MANET Attacks

Mohamed A. Abdelshafy, Peter J. B. King
School of Mathematical & Computer Sciences
Heriot-Watt University
Edinburgh, UK
{ma814, P.J.B.King}@hw.ac.uk

Abstract

AODV is a well-known reactive protocol designed for MANET routing. All MANET routing protocols are designed based on the assumption that all nodes cooperate without maliciously disrupting the operation of the routing protocol. A large number of attack types of varying severity are threatening MANET. In this paper, we study the performance of AODV routing protocol in the presence of some of the well-defined attacks in MANET. We use NS-2 network simulator to analyse the impacts of blackhole, grayhole, selfish and flooding attacks on AODV protocol performance. While the blackhole and flooding attacks have a severe impact on the AODV performance, the selfish and grayhole attacks have less significant effect on it.

1. Introduction

Routing protocols in a Mobile Ad Hoc Network (MANET) are designed based on the assumption that all nodes are cooperating to forward data from a source to a destination. So, each node in a MANET acts both as a router and as a host. A large number of routing protocols that are designed to optimize the network performance for MANETs [4] have been developed over the past years. The major issues involved in designing a routing protocol for MANET are node mobility, bandwidth constrained and error prone wireless channel, resource constrained nodes, and dynamic changing of the network topology [1].

MANET routing protocols can be classified as proactive or reactive protocols. In proactive (table-driven) routing protocols, each node maintains one or more tables containing routing information to every other node in the network. On the other hand, reactive (on-demand) routing protocols, routes are only created when a source requires to send data to a destination node which means that these protocols are initiated by a source on-demand. In this paper, we focus on AODV routing protocol [9] as it is one of the well-known and extensively studied reactive protocols chosen by the IETF for standardization.

MANET routing protocols are designed based on the assumption that all nodes cooperate without maliciously disrupting the operation of the protocol and do not provide defense against malicious nodes [1]. However, the presence of malicious nodes cannot be ignored in MANETs because of the wireless nature of the network and the mobility of nodes that adds a difficulty of distinguishing between stale routes and fake routes. Nodes in MANET have limited computation and power capabilities that introduce a difficulty to implement cryptography and key management algorithms which require high computations. A malicious node can attack the network layer in MANET either by not forwarding packets or by changing some parameters of routing messages such as sequence number and IP addresses, sending fake messages several times and sending fake routing information to disrupt routing operations [1]. While there is large number of existing attacks, our paper is focused on flooding, grayhole, selfish and blackhole attacks.

The rest of the paper is organized as follows. In section 2, an overview of the AODV routing protocol is presented and the impact of some attacks on MANET is discussed. In section 3, the simulation approach and parameters are presented. In section 4, simulation results are given. In section 5, concluding remarks are introduced.

2. Attacking AODV Protocol

Ad Hoc On-Demand Vector Routing (AODV) [9] is a reactive routing protocol. It uses destination sequence numbers to ensure the freshness of routes and guarantee loop freedom. Routing information is stored only in the source node, the destination node, and the intermediate nodes along the active route which deal with data transmission. To find a path to a destination, a node broadcasts a route request (RREQ) packet to its neighbors using a new sequence number. Each node that receives the broadcast sets up a reverse route towards the source of the RREQ unless it has a fresher one. When the destination or an intermediate node that has a fresh route to the destination receives the RREQ, it unicasts a reply by sending a route reply (RREP) packet along the reverse path established at intermediate nodes during the route discovery process. Then the source node starts sending data packets to the destination node through the neighboring node that first responded with an RREP. If a link is broken during transmission, an upstream neighbor sends a route error (RERR) packet to its affected neighbors.

2.1.AODV under Flooding Attack

In a flooding attack [6], a malicious node floods the network with a large number of RREQs to non-existent destinations in the network which drains a lot of the network resources. Since the destination does not exist in the network, a RREP packet cannot be generated by any node in the network and all nodes keep on disseminating the RREQ packet. This can introduce a difficulty to create new routes and to transmit data packets specially when a large number of fake RREQ packets are broadcast into the network. Thus, it leads to congestion in the network and overflow of route table in the intermediate nodes so that the nodes cannot receive new RREQ packet, resulting in a DoS attack. Moreover, unnecessary forwarding of these fake RREQ packets consumes computational and power resources of nodes which are limited in MANET [3].

2.2.AODV under Selfish Attack

In a selfish attack [5], a selfish node is the node that saves its resources; such as battery, by not cooperating in the network operations. A selfish node affects the network performance as it does not correctly process routing or data packets based on the routing protocol. The selfish node does not even send HELLO messages and drops all data and control packets even if these packets are sent to it. When a selfish node needs to send data to another node, it starts working as normal AODV operation. After it finishes sending its data, the node returns to its silent mode and the selfish behavior by dropping all data and routing packets directed through it. Neighbor nodes detect the absence of the selfish node after an interval of silence, and will assume that the node has left their neighborhood. So, they invalidate their own route entries to this node and selfish node becomes invisible to the network. The selfish node behavior is known as a selective existence attack and it is a kind of a passive attack as the node neither participates in the network operation nor changes the content of packets.

2.3.AODV under Grayhole Attack

In a grayhole attack [7], a malicious node behaves normally as a truthful node during the route discovery process by replying with true RREP packets to the nodes that started RREQ packets. After the source node starts sending data through the malicious node, the malicious node starts dropping these data packets to launch a denial of service (DoS) attack. So, the malicious node forwards routing packets and drops data packets. This selective dropping makes grayhole attacks much more difficult to detect than blackhole attacks. Grayhole attack is also known as node misbehaving attack [2] as the malicious node misleads the network by agreeing to forward the packets in the network.

2.4.AODV under Blackhole Attack

In a blackhole attack [10], a malicious node absorbs the network traffic and drops all packets. Once the malicious node receives an RREQ packet, without checking its routing table, it immediately sends a false RREP packet with a high sequence number and hop count equals 1 to spoof its neighbours that it has the best route to the destination. Thus, the malicious node reply will be received by the source node before any reply from other nodes. Complying with the normal AODV operation, a source node which receives multiple RREP chooses the RREP with the largest destination sequence number and the smallest hop count. Therefore, the source node ignores other RREP packets and begins sending data packets through the malicious node. When the data packets routed by the source node reach the malicious node, it drops these data packets rather than forwarding them to the destination node. The malicious node attacks all RREQ packets in this way and takes over all routes. Therefore all packets are sent to a point where they are not forwarding anywhere.

3. Simulation Approach

NS-2 simulator [8] is used to simulate grayhole, blackhole, flooding and selfish attacks. The simulation is used to analyse the performance of AODV routing protocol under these attacks. The parameters used are shown in Table I. Node mobility was modelled with the random waypoint method. Our simulation results are obtained from 3 different movement scenarios, 3 different traffic scenarios and 3 different node-type (malicious or non-malicious) scenarios which means that each metric value is the mean of the 27 runs. The node-type scenario is created randomly. In all cases, the 90% confidence interval was small compared with the values being reported. While we examined the effects of the attacks on both UDP and TCP traffic, this paper is focused on their impact on the TCP traffic only. We also examined the effect of these attacks for different node speeds (0, 5, 10, 15, 20, 25 and 30 m/s). Our analysis shows that the node mobility has no significant effect on the protocol performance in the presence of malicious nodes. So, the paper results are focused only on the static network (0 m/s) and a high mobility network (30 m/s).

TABLE I. SIMULATION PARAMETERS

Simulation Time	180 s
Simulation Area	1000 m x 1000 m
Number of Nodes	100
Number of Connections	70
Number of Malicious Nodes	0 - 5
Node Speed	0 - 30 m/s
Pause Time	10 s
Traffic Type	TCP

Packet Delivery Ratio (PDR): The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by a source.
Throughput: The number of data bits delivered to the application layer of a destination node in unit time measured in bps.
End-to-End Delay (EED): The average time taken for a packet to be transmitted across the network from a source to a destination.
Routing Overhead: The number of routing packets for route discovery and route maintenance needed to deliver the data packets from sources to destinations.
Normalized Routing Load (NRL): The total number of routing packets transmitted divided by the number of received data packets.
Route Discovery Latency (RDL): The average delay between the sending RREQ from a source and receiving the first

corresponding RREP.
Sent Data Packets: The total number of packets sent by all source nodes during the simulation time.

4. Simulation Results

4.1.AODV under Flooding Attack

Figure 1 shows the effect of malicious nodes on the packet delivery ratio for static nodes and for high node mobility. The result shows that the packet delivery ratio decreases while increasing the number of malicious nodes in the network and this decrease is independent of the node mobility. The graph shows that while the PDR decreases by 3% if there are 5 malicious nodes for static nodes, the PDR decreases by 5.5% for the same number of malicious nodes in high node mobility.

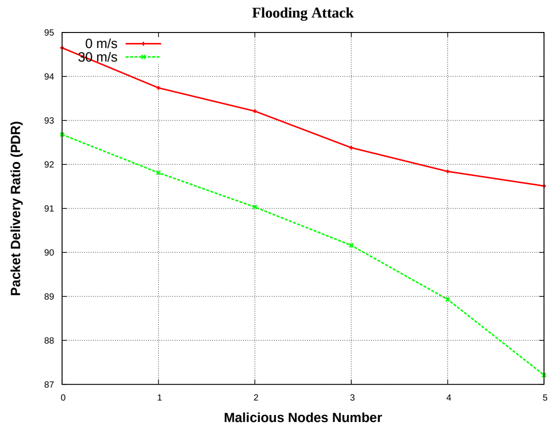

Figure 1. PDR under Flooding Attack

Figure 2 shows the effect of malicious nodes on the network throughput. The result shows that the throughput decreases by 10% for each malicious node introduced in the network and this decrease is independent of the node mobility.

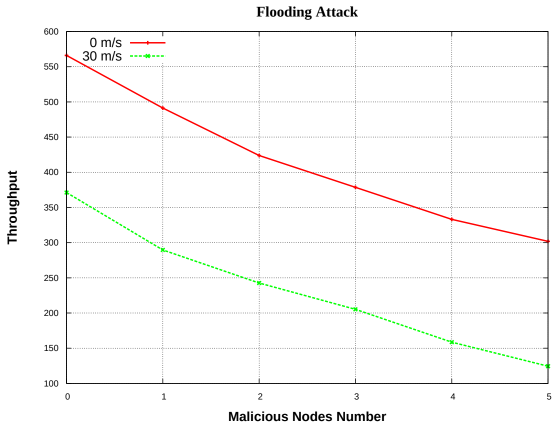

Figure 2. Throughput under Flooding Attack

The effect of malicious nodes on the end-end-delay is shown in Figure 3. The result shows that the delay has no significant change for the first malicious node while the delay increases as more malicious nodes are added in the network up to 30% in the average if there are 5 malicious nodes and this increase is independent of the node speed.

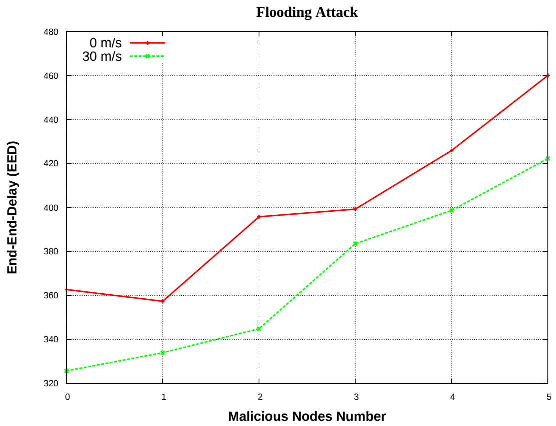

Figure 3. EED under Flooding Attack

Figure 4 shows the effect of malicious nodes on the routing overhead. The result shows that the routing overhead linearly increasing by 50% in the average as the number of malicious nodes in the network increases for static nodes while the increase is about 70% for high node mobility.

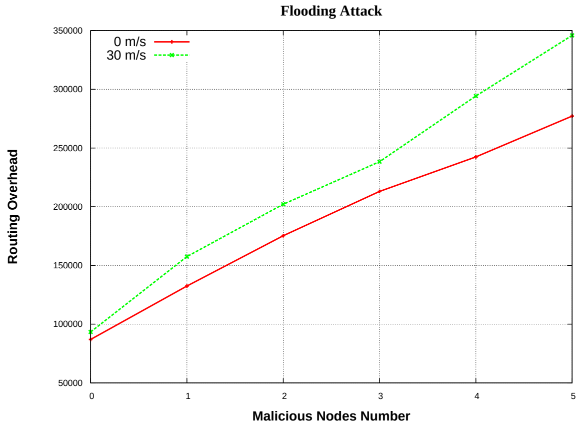

Figure 4. Routing Overhead under Flooding Attack

The effect of malicious nodes on the normalized routing load is shown in Figure 5. For static network, NRL increases linearly by 80% for each added malicious node. With high mobile nodes, the increase is about 100% for each added malicious node, which is more obvious for large number of malicious nodes.

The effect of malicious nodes on the routing discovery latency is shown in Figure 6. The result shows that RDL increases for each malicious node introduced in the network and this increase is independent of the node mobility. For small number of malicious nodes, RDL is less for high mobile

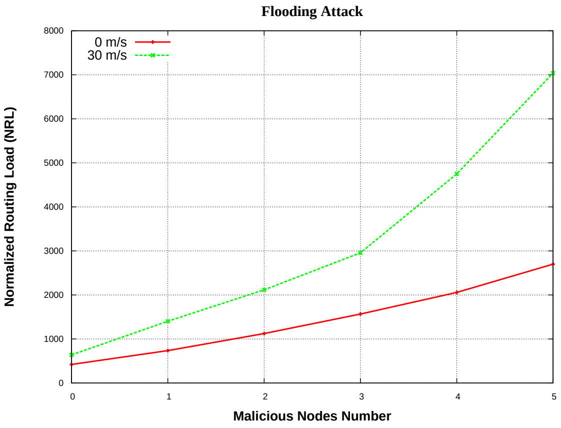

Figure 5. NRL under Flooding Attack

nodes, but as the number of malicious nodes increases, the highly mobile network will display a higher RDL than a static network.

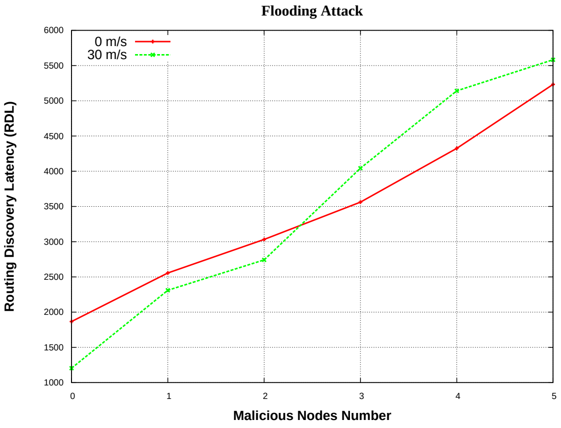

Figure 6. RDL under Flooding Attack

Figure 7 shows the effect of malicious nodes on the total number of packets sent by all sources. The result shows that the total number of data packets sent by all the source nodes decreases by 10% for each malicious node introduced in the network and this decrease is independent of the node mobility.

4.2.AODV under Selfish Attack

Figure 8 shows the effect of malicious nodes on the packet delivery ratio. The result shows that the packet delivery ratio has no significant change as the number of malicious nodes increases in the network and this is independent of the node mobility.

Figure 9 shows the effect of malicious nodes on the network throughput. The result shows that while the throughput of high mobility nodes decreases by 40% relative to the static nodes, the throughput has no significant change as the number of malicious nodes increases.

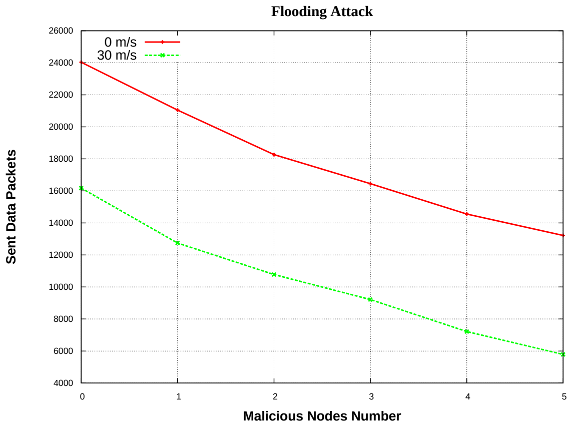

Figure 7. Sent Data under Flooding Attack

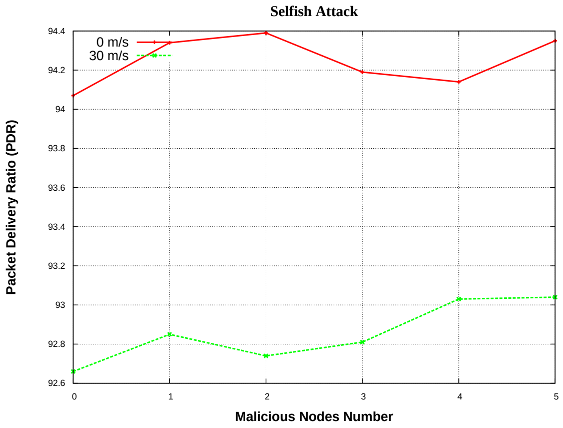

Figure 8. PDR under Selfish Attack

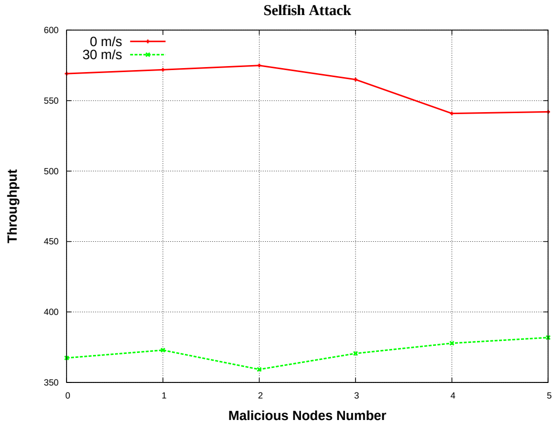

Figure 9. Throughput under Selfish Attack

The effect of malicious nodes on the end-end-delay is shown in Figure 10. The result shows that the delay has no significant change as the number of malicious nodes increases in the network and this is independent of the node mobility. In addition, the delay for static network is better than for high mobility nodes by approximately 10%.

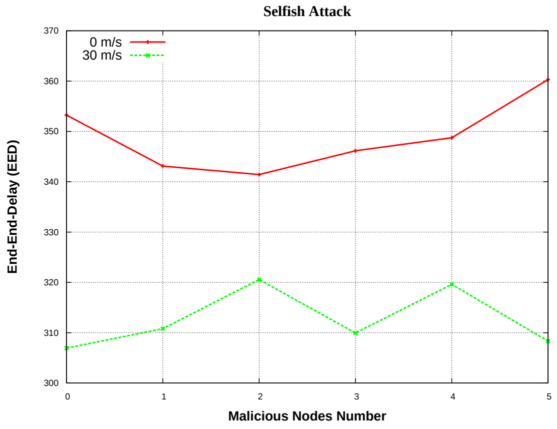

Figure 10. EED under Selfish Attack

Figure 11 shows the routing overhead under the selfish attack as the number of malicious nodes increases. For the static network, the first two malicious nodes have little effect; and adding future malicious nodes reduces the overhead slightly. In the highly mobile network, there is a significant reduction in overhead for each malicious node added. These results are slightly confusing as the selfish attack improves the routing overhead. This is because the selfish nodes drops and does not rebroadcast all received RREQ which decreases routing overhead.

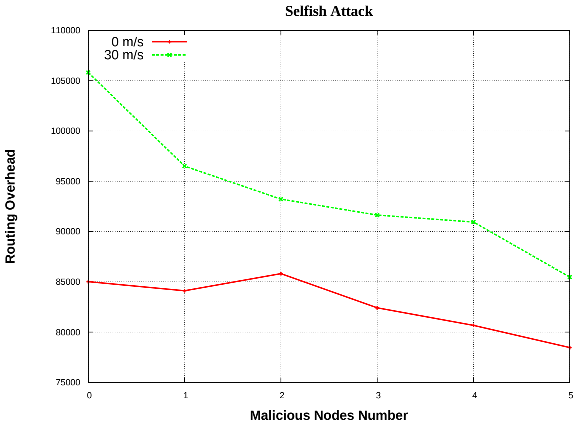

Figure 11. Routing Overhead under Selfish Attack

The effect of malicious nodes on the normalized routing load is shown in Figure 12. The result shows that while NRL has no significant change in the case of static nodes, it decreases by 5% on the average for each malicious node in the case of high mobility nodes. Because the number of routing packets affects NRL, NRL is slightly improved as the number of malicious nodes increases.

The effect of malicious nodes on the routing discovery latency is shown in Figure 13. The result shows that RDL for the high mobility nodes is better than the static nodes by 25% on the average regardless the number of malicious nodes in the network.

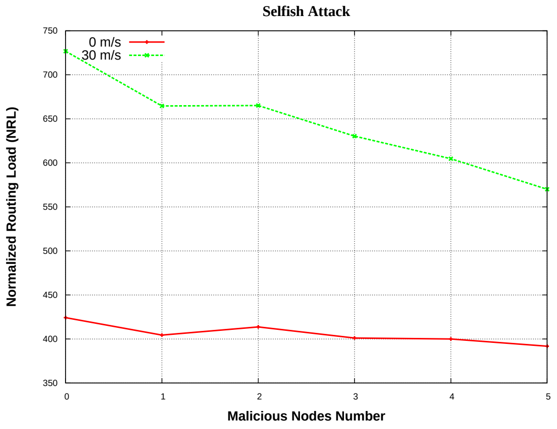

Figure 12. NRL under Selfish Attack

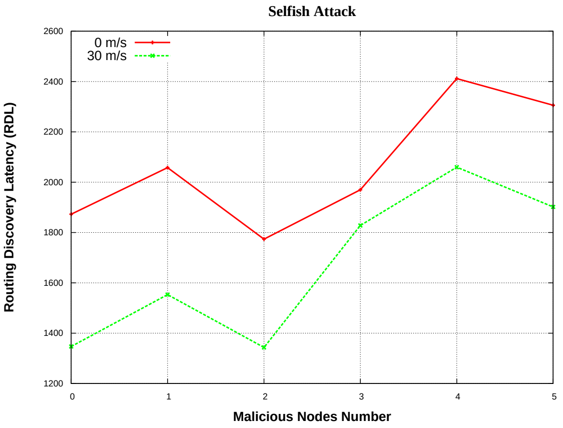

Figure 13. RDL under Selfish Attack

Figure 14 shows the effect of malicious nodes on the total number of packets sent by all sources. The result shows that the total number of data packets sent by all the source nodes has no significant change as a results of malicious nodes presence in the network and this is independent of the node mobility. Moreover, static nodes can send approximately 150% data packets than highly mobile nodes.

4.3.AODV under Grayhole Attack

As the grayhole node drops all data packets and the selfish node drops all data and routing packets, the grayhole attack simulation produces very similar results to the selfish attack. This is because of the packet delivery ratio, network throughput, end-end-delay, normalized routing load and routing overheads are calculated based on the received data packets which are identical for the same simulation scenario.

Figure 15 shows the effect of malicious nodes on the packet delivery ratio. The result shows that the packet delivery ratio has not changed significantly as the number of malicious nodes in increased in the network and this is independent of the node mobility.

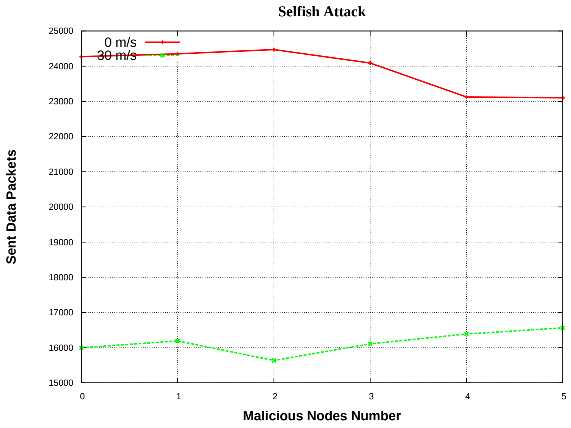

Figure 14. Sent Data under Selfish Attack

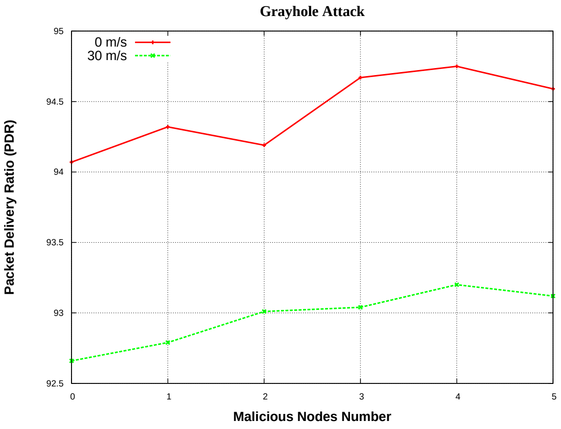

Figure 15. PDR under Grayhole Attack

Figure 16 shows the effect of malicious nodes on the network throughput. The result shows that while the throughput of high mobility nodes decreases by 35% relative to the static nodes, the throughput is not affected by the number of malicious nodes in the network.

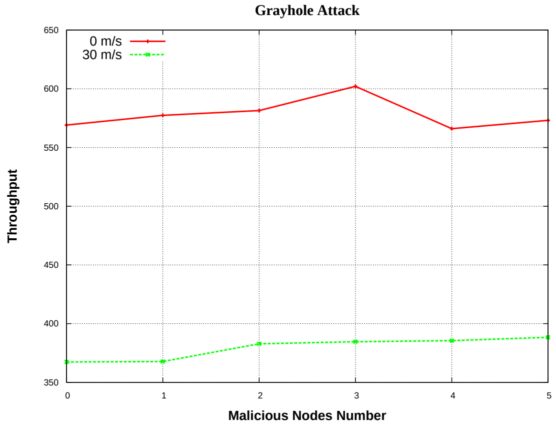

Figure 16. Throughput under Grayhole Attack

The effect of malicious nodes on the end-end-delay is shown in Figure 17. The result shows that the delay of high mobility nodes is better than static nodes by 10% and the delay is not affected by the number of malicious nodes in the network.

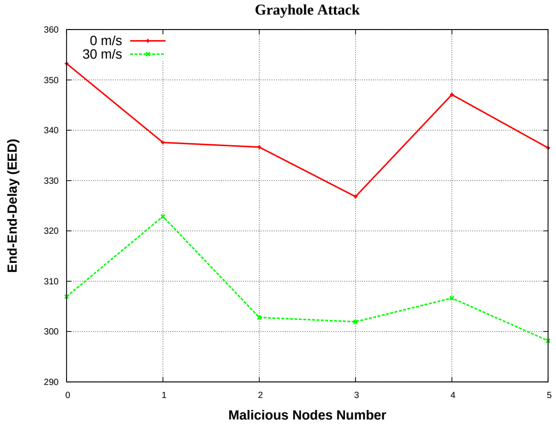

Figure 17. EED under Grayhole Attack

Figure 18 shows the effect of malicious nodes on the routing overhead. The result shows that the routing overhead for static nodes is better than its value in high mobility nodes by about 10% and while it decreases by 5% for each malicious node in the case of high mobility nodes, the routing overhead decreases by 3% for each malicious node in the case of static nodes. This confusing enhancement as discussed in selfish attack is a result of dropping RREQ packets by the malicious nodes.

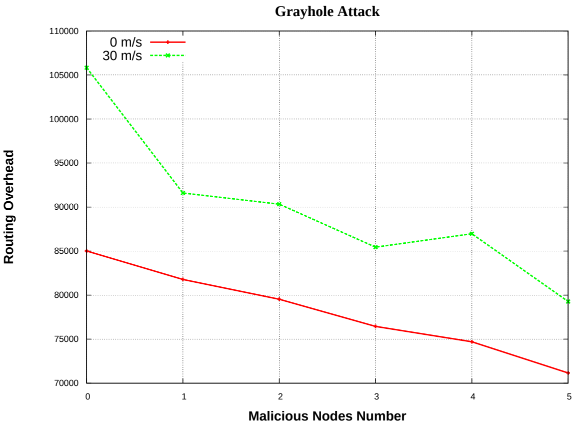

Figure 18. Routing Overhead under Grayhole Attack

The effect of malicious nodes on the normalized routing load is shown in Figure 19. The result shows that NRL for static nodes is better than its value in high mobility nodes by about 40% and while it decreases by 6% for each malicious node in the case of high mobility nodes, the routing overhead decreases by 4% for each malicious node in the case of static nodes. Because the number of routing packets affects NRL, NRL is slightly improved as the number of malicious nodes increases.

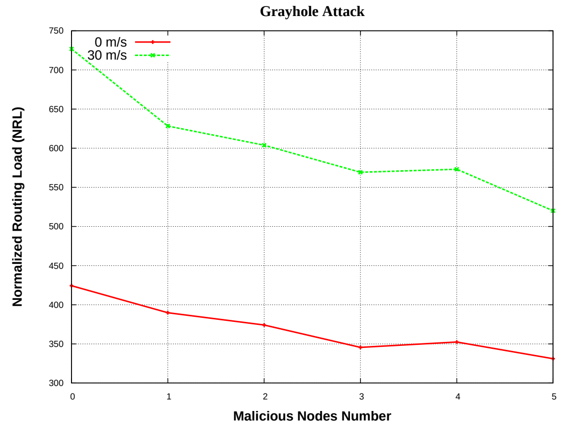

Figure 19. NRL under Grayhole Attack

The effect of malicious nodes on the routing discovery latency is shown in Figure 20. The result shows that RDL for the high mobility nodes is better than the static nodes by 20% on the average regardless the number of malicious nodes in the network.

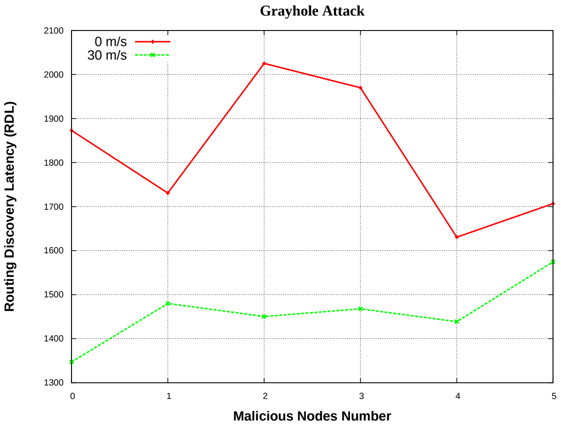

Figure 20. RDL under Grayhole Attack

Figure 21 shows the effect of malicious nodes on the total number of packets sent by all sources. The result shows that the total number of data packets sent by all source nodes has no significant change as a result of presence of malicious nodes in the network and this is independent of the node mobility. Moreover, static nodes can send approximately 150% data packets than highly mobile nodes.

4.4.AODV under Blackhole Attack

Figure 22 shows the effect of malicious nodes on the packet delivery ratio. The result shows that the packet delivery ratio has no significant change for the first malicious node while the packet delivery ratio decreases by about 6% for each malicious node in the network and this decrease is independent of the node mobility.

Figure 23 shows the effect of malicious nodes on the network throughput. The result shows that the throughput for static nodes is better than its value in high mobility nodes by 15% and the throughput decreases by 20% for each malicious node introduced in the network and this decrease is independent of the node mobility.

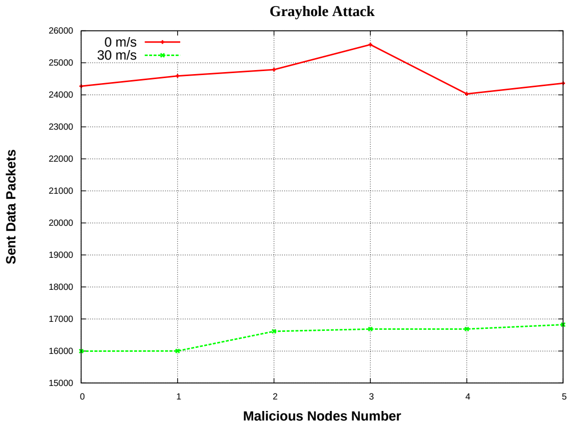

Figure 21. Sent Data under Grayhole Attack

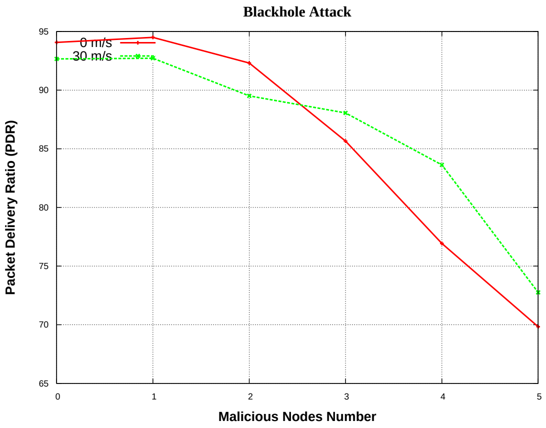

Figure 22. PDR under Blackhole Attack

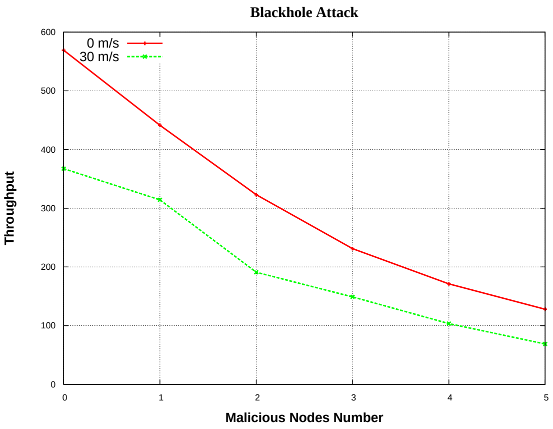

Figure 23. Throughput under Blackhole Attack

The effect of blackhole attack on the end-end-delay is shown in Figure 24. The first two malicious nodes reduce the delay significantly; independently of whether the network is static or highly mobile. Subsequent malicious nodes decrease the delay by fewer ratios. While the results show that the delay is reduced as the number of malicious nodes increases which is slightly paradoxical as the attack improves the delay. This is a misleading result because the delay is only measured on packets that reach their destinations and since the blackhole nodes drop all the received data, the number of packets that will be considered in calculating the delay decreases as the number of malicious nodes increases. So, the routes that avoid blackhole nodes suffer less competition, and hence reduced delay.

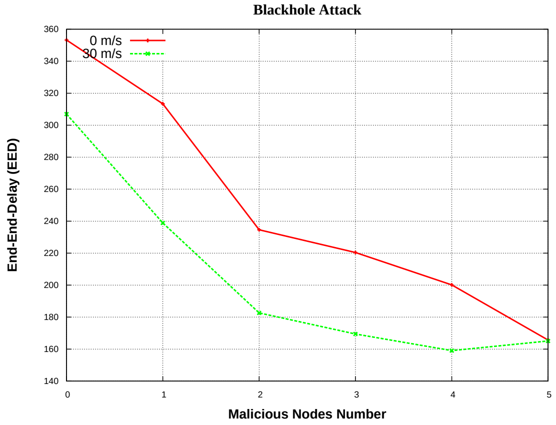

Figure 24. EED under Blackhole Attack

Figure 25 shows the effect of malicious nodes on the routing overhead. The result shows that the routing overhead has not significant change as a result of malicious nodes presence in the network and this is independent of the node mobility. These results have slightly confusion as the blackhole attack improves the routing overhead. As mentioned before, the explanation of the confusion of routing overhead enhancement as the number of malicious nodes increases is because the malicious nodes drop all received RREQ.

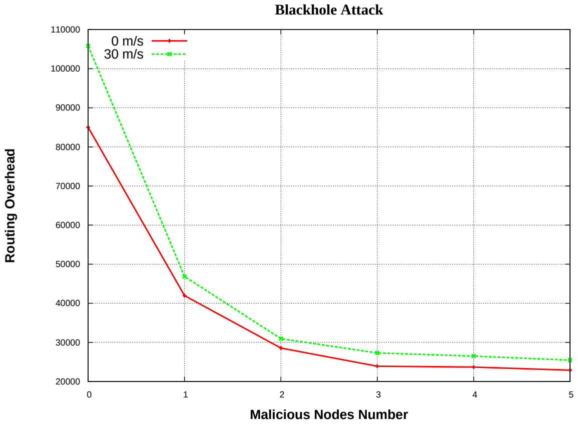

Figure 25. Routing Overhead under Blackhole Attack

The effect of malicious nodes on the normalized routing load is shown in Figure 26. The result shows that the first three malicious nodes have very little impact on the NRL while the presence of other malicious nodes dramatically increases NRL. While this conclusion is true for both mobile and static node, the effect on static node is more remarkable.

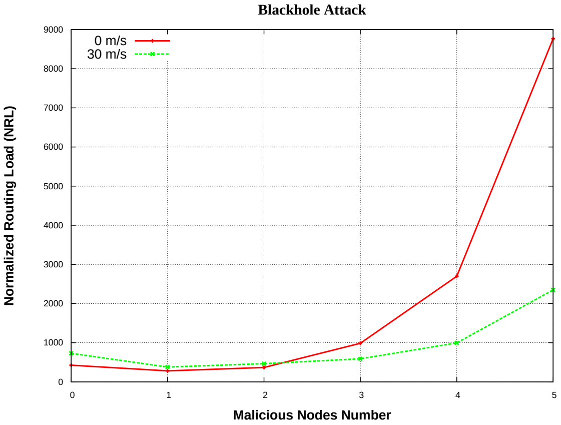

Figure 26. NRL under Blackhole Attack

The effect of malicious nodes on the routing discovery latency is shown in Figure 27. While the result shows that RDL decreases dramatically for each malicious node introduced in the network which is a positive sign, this is a deceptive advantage because RDL is computed based on the difference between RREQ and RREP times. Since a malicious node under blackhole attack replies with a fake RREP, RDL becomes smaller under attack.

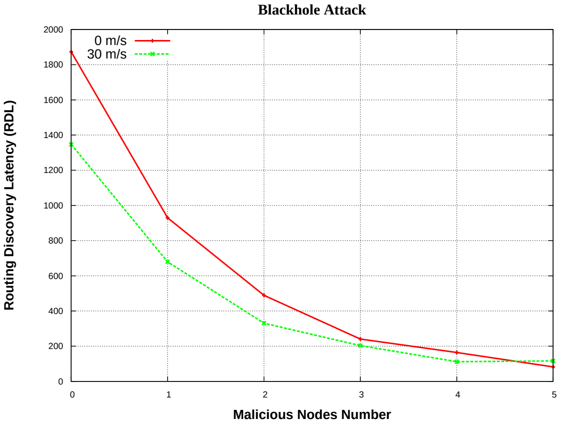

Figure 27. RDL under Blackhole Attack

Figure 28 shows the effect of malicious nodes on the total number of packets sent by all sources. The result shows that the total number of data packets sent by all source nodes increases in static nodes by 30% than in high mobility nodes and these packets decreases by 15% for each malicious node introduced in the network and this decrease is independent of the node mobility.

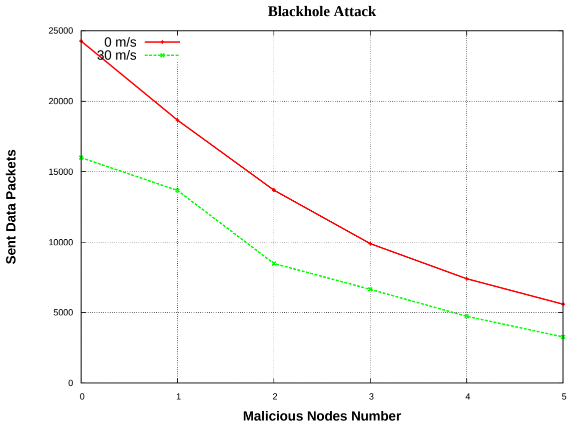

Figure 28. Sent Data under Blackhole Attack

5. Conclusion

In this paper, we study the behavior of flooding, selfish, grayhole and blackhole attacks on AODV routing protocol using NS-2 network simulator. Analysing the impact of these attacks on the performance metrics such as packet delivery ratio, network throughput, end-end-delay, routing overhead, normalized routing load, routing discovery latency and sent data packets is investigated.

From the simulation, we conclude that the blackhole and flooding attacks have dramatic impact on the network performance. The blackhole introduces a fake RREP which affects the network performance and the flooding attack introduces a fake RREQ which affects the network performance as well. As most of the performance metrics depend on the number of received data packets, little change is observed in these metrics under grayhole and selfish attack because the malicious nodes drop data packets in these attacks.

References

[1] M. Abdelshafy and P. J. B. King. Analysis of security attacks on aodv routing. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, pages 1–6, London, UK, 2013.

[2] M. Arya and Y. K. Jain. Grayhole attack and prevention in mobile adhoc network. *International Journal of Computer Applications*, 27(10):21–26, August 2011.

[3] A. Bandyopadhyay, S. Vuppala, and P. Choudhury. A simulation analysis of flooding attack in MANET using ns-3. In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*, pages 1–5, 2011.

[4] A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. Bölöni, and D. Turgut. Routing protocols in ad hoc networks: a survey. *Computer Networks*, 55(13):3032–3080, September 2011.

[5] P. Goyal, S. Batra, and A. Singh. A literature review of security attack in mobile ad-hoc networks. *International Journal of Computer Applications*, 9(12):11–15, November 2010.

[6] Y. Guo and S. Perreau. Detect DDoS flooding attacks in mobile ad hoc networks. *Int. J. Secur. Netw.*, 5(4):259–269, Dec. 2010.

[7] K. Manikandan, R.Satyaprasad, and K.Rajasekhararao. A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks. *IJACSA - International Journal of Advanced Computer Science and Applications*, 2(3):7–12, 2011.

[8] The network simulator ns-2. http://www.isi.edu/nsnam/ns/.

[9] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, 1997.

[10] N. Sharma and A. Sharma. The black-hole node attack in MANET. In *Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies*, ACCT '12, pages 546–550, Washington, DC, USA, 2012. IEEE Computer Society.